INTRODUCTION

Public safety personnel are often positioned to identify suspicious activity potentially related to terrorism, and in some cases, first responders who have reported this information have helped to disrupt terrorist plans or attacks in the US. **JCAT'S COUNTERTERRORISM GUIDE FOR PUBLIC SAFETY PERSONNEL** is designed to assist first responders in:

- **RECOGNIZING** and **REPORTING** suspicious activity that may be linked to terrorism, consistent with the Nationwide Suspicious Activity Reporting (SAR) Initiative;

- **SPOTTING** indicators of mobilization to violence; and,
- **RESPONDING** to and **MITIGATING** terrorist attacks.

THE GUIDE IS DERIVED FROM EXISTING UNCLASSIFIED SOURCES.

COUNTERTERRORISM PARTNERS = ENHANCED INFORMATION SHARING

JOINT TERRORISM TASK FORCES (JTTFs) serve as the coordinated “action arms” for federal, state, and local government response to terrorism threats in specific US geographic regions. The FBI is the lead agency that oversees JTTFs. The benefits of a JTTF include:

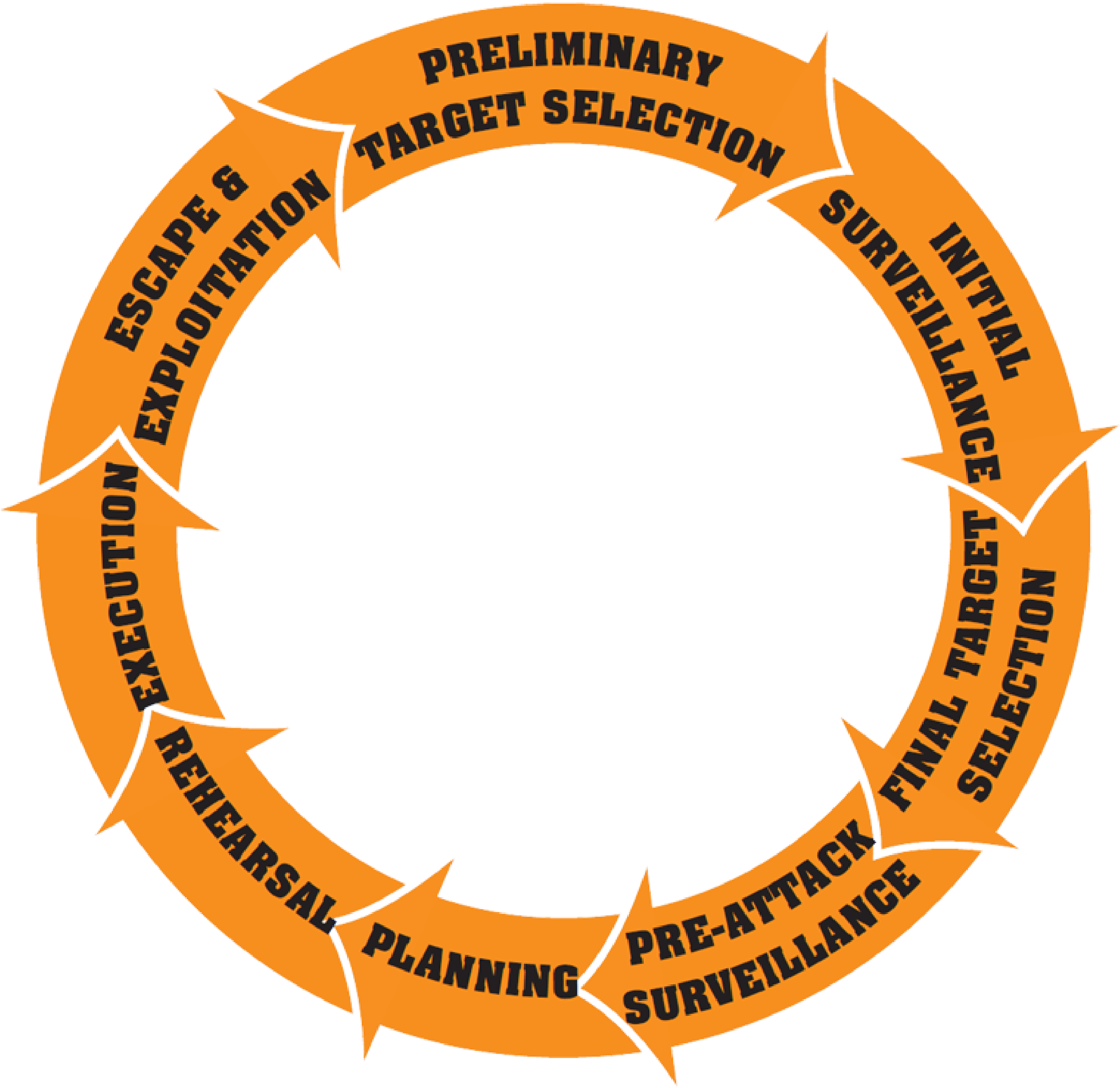
- “One-stop shopping” for law enforcement information or investigation of suspected or real terrorist activities
- Use of a shared intelligence base
- Ability to prosecute cases in the jurisdiction that is most efficient and effective
- Task force member awareness of investigations within a jurisdiction and ability to assist in investigations in other jurisdictions
- Familiarity among agencies, investigators, and managers before a crisis occurs

The mission of a JTTF is to leverage the collective resources of the member agencies for the prevention, preemption, deterrence, and investigation of terrorist acts that affect US interests, to disrupt and prevent terrorist acts, and to apprehend individuals who may commit or plan to commit such acts. To further this mission, a JTTF serves as a means to facilitate information sharing among JTTF members.

FUSION CENTERS are defined as a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing the ability to detect, prevent, investigate, and respond to criminal and terrorism activity *(Fusion Center Guidelines, August 2006)*. The fusion centers are owned and operated by state and local governments with support from federal partners. Although fusion centers predate the 9/11 terrorist attacks, the concept gained momentum and was promoted by state and local law enforcement and homeland security officials during post-9/11 discussions as a more effective way to protect their communities.

TERRORIST ATTACK PLANNING CYCLE

Understanding the terrorist attack planning cycle can help first responders and public safety personnel recognize preoperational activities. Terrorists generally plan attacks in observable stages, although specific details, sequencing, and timing can vary greatly and change over time. Preattack surveillance, training, and rehearsals are the stages of the planning cycle that are often observable and can offer opportunities to identify plots and prevent attacks.



REPORTING SUSPICIOUS ACTIVITY

> “WHETHER A PLAN FOR A TERRORIST ATTACK IS HOMEGROWN OR ORIGINATES OVERSEAS, IMPORTANT KNOWLEDGE THAT MAY FOREWARN OF A FUTURE ATTACK MAY BE DERIVED FROM INFORMATION GATHERED BY STATE, LOCAL, AND TRIBAL GOVERNMENT PERSONNEL IN THE COURSE OF ROUTINE LAW ENFORCEMENT AND OTHER ACTIVITIES.”

NATIONAL STRATEGY FOR INFORMATION SHARING OCTOBER 2007

THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING (SAR) INITIATIVE (NSI) is a joint collaborative effort by DHS, FBI, and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.

Online SAR Training for Law Enforcement and Hometown Security Partners: the NSI training strategy is a multifaceted approach designed to increase the effectiveness of state, local, and tribal law enforcement and public safety professionals and other frontline partners in identifying, reporting, evaluating, and sharing preincident terrorism indicators to prevent acts of terrorism. The SAR Line Officer Training and each sector-specific SAR Hometown Security Partners Training discuss how to report identified suspicious activity to the proper authorities while maintaining the protection of citizens’ privacy, civil rights, and civil liberties.

Online training is available on the NSI website (http://nsi.ncirc.gov/training_online.aspx (http://nsi.ncirc.gov/training_online.aspx)) and includes:

- Scenarios that illustrate the benefit and importance of SAR
- Descriptions of SAR-related behaviors and indicators
- A certificate of completion

INDICATORS OF SUSPICIOUS ACTIVITY

ONE OR MORE OF THESE INDICATORS COULD SIGNAL SUSPICIOUS ACTIVITY, ALTHOUGH EACH SITUATION MUST BE INDEPENDENTLY EVALUATED. WHEN THE BEHAVIOR OR ACTIVITY INVOLVES BEHAVIORS THAT MAY BE LAWFUL OR IS CONSTITUTIONALLY PROTECTED ACTIVITY, THE INVESTIGATING LAW ENFORCEMENT AGENCY WILL CAREFULLY ASSESS THE INFORMATION AND GATHER AS MUCH INFORMATION AS POSSIBLE BEFORE TAKING ANY ACTION, INCLUDING DOCUMENTING AND VALIDATING THE INFORMATION AS TERRORISM-RELATED AND SHARING IT WITH OTHER LAW ENFORCEMENT AGENCIES.

POTENTIAL CRIMINAL OR NONCRIMINAL ACTIVITIES REQUIRING ADDITIONAL INFORMATION DURING INVESTIGATION

ELICITING INFORMATION: Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.

TESTING OF SECURITY: Interactions with or challenges to installations, personnel, or systems that reveal physical, personnel, or cyber security capabilities.

- Unscheduled deliveries of materials or equipment.
- Unattended or unauthorized vessels or vehicles in unusual or restricted areas.
- Overt testing of security measures or emergency response.

RECRUITING: Building operations teams and contacts, personnel data, banking data, or travel data.

OBSERVATION/SURVEILLANCE: Demonstrating unusual attention to facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, or attempting to measure distances.

PHOTOGRAPHY: Taking photos or videos of facilities, buildings, or infrastructure in a questionable manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), or security-related equipment (perimeter fencing, security cameras), etc. All reporting should be done within the totality of the circumstances.

MATERIALS ACQUISITION/STORAGE: Procurement of unusual quantities of possible IED materials, such as cellphones, pagers, fuel, or timers, and/or explosive precursors, such as fertilizers, fuels, or acids, such that a reasonable person would suspect possible criminal activity.

- Hidden, disguised, or unusual storage of:
  » Laboratory equipment—Bunsen burners, lab stands, and scientific glassware.
  » Personal protective equipment—masks, goggles, and gloves.
  » Household items—strainers, coffee grinders, and filters.
  » Common household chemicals—acetone, peroxide, and sulphuric acid (e.g. drain cleaner).
- Attempted purchase of controlled materials without proper credentials.
- Attempted purchase of controlled or hazardous materials in bulk quantities.
- Presence of potential precursors for chemical or biological agent production.
- Individual has little knowledge of intended purchase items.
- Possession of instructions to create potentially harmful devices, chemicals, or agents.

ACQUISITION OF EXPERTISE OR CAPABILITY: Attempts to obtain or conduct training in security concepts (military weapons or tactics) or other unusual capabilities that would arouse suspicion in a reasonable person.

- Interest in using or modifying technology for uses outside of intended purpose.

WEAPONS DISCOVERY: Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.

- Discovery of homemade explosive precursor, such as fertilizers, strong acids, peroxides, and solvents.
- Discovery of chemical or biological precursors, such as anhydrous ammonia, sulfur, castor beans, acetone, and Epsom salt.
- Items found onsite that do not belong or otherwise seem out of place.
- Burn marks or discoloration on walls, doors, ground, and/or floor; presence of unusual odors or liquids.
- Unusual or unpleasant odors, chemical fires, brightly colored stains, or corroded or rusted metal fixtures in otherwise dry and weather-protected environments.
- Chemical burns on hands or body, chemical bleaching of skin or hair.
- Injuries or illness inconsistent with explanation.

SECTOR-SPECIFIC INCIDENT: Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector) with regard to their personnel, facilities, systems, or functions.

BREACH/ATTEMPTED INTRUSION: Unauthorized personnel attempting to enter or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g., police/security, janitor).

- Access badge sharing and “piggy backing” at security gates and doors.
- Seeking additional access to or encountered within restricted or controlled areas.
- Attempting to acquire official vehicles, uniforms, identification, and access cards.

MISREPRESENTATION: Presenting false or misusing insignia, documents, and/or identification to misrepresent one’s affiliation to cover possible illicit activity.

- Refusal to provide all required information when completing paperwork.
- Forged or altered identification.
- Use of fraudulent documents (often referred to as “breeder” documents), which may be used to obtain official documents, including birth/death certificates, drivers licenses, and passports.

THEFT/LOSS/DIVERSION: Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents [classified or unclassified]) that are proprietary to the facility.

- Hazardous materials or controlled substances.

SABOTAGE/TAMPERING/VANDALISM: Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.

CYBER ATTACK: Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.

EXPRESSED OR IMPLIED THREAT: Communicating a spoken or written threat to damage or compromise a facility/infrastructure.

- Against the US or individuals.

AVIATION ACTIVITY: Operation of an aircraft in a manner that reasonably may be interpreted as suspicious or posing a threat to people or property. This activity may or may not be in violation of Federal Aviation Regulations.

PRECURSORS OF VIOLENT EXTREMISM

AT THE STATE AND LOCAL LEVEL, THE IMPORTANCE OF A WHOLE OF GOVERNMENT APPROACH TO STEMMING HOMEGROWN VIOLENT EXTREMISM, INCLUDES THE LOCAL COMMUNITY AND ITS FIRST RESPONDERS.

Communities are an integral part of the effort to prevent violent extremism and can assist law enforcement in identifying at-risk individuals. Awareness and vigilance are crucial to identify behaviors that can lead to a violent act. Several behaviors, when taken in context, can indicate radicalized individuals are mobilizing—preparing to engage in violence to advance their cause. These behaviors include seeking out training, building capability, and other preparatory behaviors. The below factors drive the mobilization process and may interact to mobilize individuals toward violence. A lack of access to some or all of these factors may cause some individuals to back away from violence or result in individuals changing their plans.

READINESS TO ACT: Individual motivation and intent that keeps the person engaged and moving toward his or her intended goal. Readiness to act can vary across time and be influenced by multiple factors—including personal will and competence, experiences while in training, and motivation gained or lost as a result of established relationships.

OPPORTUNITY: Access to training and resources that provide individuals or groups the chance to take action. This can range from target practice at a local firing range to explosives training with terrorists overseas. Opportunity can also include having available time to engage in violent activities.

CAPABILITY: Training that has prepared an individual to follow through on his or her intentions. The individual's capability also includes his or her educational training and skill set acquired through life experiences.

TARGETS: Locations that the individual is familiar with because of where he or she lives or works or is interested in because of what they represent, such as supposed economic, political, or military dominance by the West.

FBI and DHS both maintain web portals which contain Countering Violent Extremism (CVE) training resources, hundreds of the most current CVE training materials, case studies, analytical products, and other resources, including preincident indicators.

For additional information, please visit DHS.GOV (http://www.dhs.gov/topic/countering-violent-extremism (http://www.dhs.gov/topic/countering-violent-extremism)), or the FBI-Countering Violent Extremism Office (FBI-CVEO) special interest group on FBI's Law Enforcement Enterprise Portal (http://www.leo.gov (http://www.leo.gov)), which house intelligence products, behavioral indicators, academic studies, and behavioral models to aid the understanding of violent extremism.

TERRORIST TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

THE FOLLOWING LIST, WHILE NOT COMPREHENSIVE, PROVIDES AWARENESS OF SELECT TTPs THAT FIRST RESPONDERS MAY ENCOUNTER AS A PRETEXT TO, IN ADVANCE OF, OR DURING CALLS FOR SERVICE.

USE OF SECONDARY EXPLOSIVE DEVICES TO TARGET FIRST RESPONDERS AND ONLOOKERS:

SECONDARY EXPLOSIVE DEVICE ATTACK TACTICS:

- After an initial attack, terrorists may try to target first responders and onlookers by detonating a second explosive device in or around the anticipated safe area or evacuation locations..

- Terrorists can conduct secondary attacks by infiltrating suicide bombers into crowds of bystanders or by detonating preset bombs remotely through the use of timers, remote triggers, or motion sensors.

- These explosive devices may be concealed in innocuous items of various sizes, such as vehicles, backpacks, garbage cans, mail boxes, and planters.

CONSIDERATIONS FOR THE IDENTIFICATION OF THREATS, EVACUATION OF HAZARDOUS AREAS, AND NOTIFICATION OF THE BOMB SQUAD:

- Secondary devices may be found in any configuration, not limited to the primary attack method.

- Maintain awareness of possible remote initiation or backup timer on any improvised explosive device.

TERRORIST IMPERSONATION OF FIRST RESPONDERS: Use of commandeered or fake Emergency Services Sector (ESS) Items could:

- Be used to gain access to secure sites.
- Be used to conduct a secondary attack.
- Create more victims, including first responders already on scene.
- Potentially affect response times and delay genuine emergency responders.
- Allow access for individuals to conduct surveillance or collect information.

SWATTING: Making a hoax 9-1-1 call to draw a response from first responders. Swatting includes spoofing or masking Caller ID information, which is legal, simple to use, and used by many businesses. There are no means available to quickly, accurately, and inexpensively identify swatting calls, so there is little choice but to dispatch resources.

DIVERSION: Tactic used to draw first responders away from the intended primary target of an attack and may be used as part of a complex or multipronged attack:

POSSIBLE INDICATORS OF DIVERSION TACTICS:

- Similar responses or suspicious activities (e.g., hoax devices or bomb threats) in multiple locations throughout the jurisdiction that disperse assets.
- Multiple responses requiring specialized or technical equipment that reduces resources.
- A significant incident or several minor incidents that require a commitment of resources to investigate or mitigate.
- Unusually high number of calls for service or incidence of activities inconsistent with typical patterns within the area of responsibility.

BEST PRACTICES IN PROTECTING FROM DIVERSIONS:

- Establish dispatch policies designed to hold resources in reserve (tiered responses).
- Provide situational updates to first responders to enhance safety.
- Ensure regular notifications to interagency partners and neighboring jurisdictions to provide shared operational picture of possible diversionary attacks.
- Plan and train for identified vulnerabilities.

USE OF STOLEN, CLONED, OR REPURPOSED VEHICLES: Cloned vehicles have been modified to resemble an authentic vehicle, and repurposed vehicles are authentic vehicles that are no longer in official service. These vehicles are typically decommissioned by departments and are publicly available for purchase at auctions or on the Internet:

- The driver or vehicle destination and origin are inconsistent with the company or service being represented.
- The driver is not knowledgeable about the company or its service.
- The driver has no uniform or has one that is inconsistent with the vehicle's advertised business.
- Vehicle registration and insurance are in named individual instead of company.
- Vehicle make, model, and year may not match company's current fleet.
- Multiple or conflicting corporate names and logos appear on the same vehicle.
- Visible identifiers, such as phone numbers, license plates, or call numbers that are inconsistent with the vehicle's operating area or mission.
- The time of day or location of vehicle that is inconsistent with its purpose.
- The vehicle appears to be heavily loaded, possibly beyond capacity.

MEDICAL DISCOVERY OF TERRORIST ACTIVITY AT THE SCENE OF A REQUEST FOR SERVICE: First responder scene size up, when combined with the totality of information received from victims, witnesses, and bystanders, offers the chance to assess whether an incident is potentially related to terrorism. First responders should remain openminded while performing medical and trauma assessments. Hastily or expediently treated injuries may be an indicator of suspicious activity, as those injured may not seek immediate medical care or use efforts to obscure the true nature of the injury.

- Trauma assessments: Explosions can result in unique injury patterns involving penetrating wounds, blunt trauma, amputations/avulsions and burns, as well as the possibility of "blast-lung." Chemical burns from contact will vary depending on the chemical type and length of exposure, while inhalation and ingestion may present a rapid onset of signs and symptoms.
- Medical assessments: Small-scale or rudimentary production of biological warfare agents may result in inadvertent human exposures, particularly among poorly trained or novice scientists working with homemade laboratory equipment. Sudden onset of symptoms may assist in determining exposure to chemical or biological agents. Multiple patients with similar chemical/biological exposure symptoms at any incident may be an indicator of suspicious activity and unexpected infections with nonendemic agents without verifiable travel exposure or unusual clusters of cases should prompt further investigation.

POSTBLAST BUILDING ASSESSMENT

During a postblast building assessment, conisder looking for the following:

- Collapse, partial collapse, or building off foundation
- Building/story noticeably leaning
- Severe cracking of walls, obvious severe damage and distress
- Ceilings, light fixtures, or other nonstructural hazards
- HazMat spills
- Stress fracture
- Bulging walls
- Sagging ceilings
- Other hazard present

WARNING: Do not enter any building structure unless fully trained and equipped for postblast hazards.

FOREIGN TERRORIST ORGANIZATIONS

AL-QA‘IDA

SOUTHEAST ASIA, NORTH AFRICA, SOMALIA, MIDDLE EAST

Usama Bin Ladin founded al-Qa‘ida in 1988 with Arabs fighting in Afghanistan against the Soviet Union. Al-Qa‘ida’s goal is to establish a pan-Islamic caliphate throughout the Muslim world by ousting Western influence and defeating Israel. On 11 September 2001, 19 al-Qa‘ida suicide attackers hijacked and crashed four US commercial jets—two into the World Trade Center, one into the Pentagon, and one into a field in Shanksville, PA—leaving nearly 3,000 people dead.

AL-QA‘IDA IN THE ARABIAN PENINSULA (AQAP)

SAUDI ARABIA, YEMEN

AQAP is a Sunni extremist group based in Yemen that orchestrated numerous high-profile terrorist attacks. Most notably, AQAP's deployment of a now-convicted Nigerian-born operative to detonate an explosive device aboard a Northwest Airlines flight on 25 December 2009—the first attack inside the US by an al-Qa‘ida–affiliated group since 11 September 2001.

AL-QA‘IDA IN THE LANDS OF THE ISLAMIC MAGHREB (AQIM)

NORTH AND WEST AFRICA

AQIM is led by Abdelmalek Droukdel and was founded in 1998 as Groupe Salafiste pours la Prédication et la Combat (GSPC), which splintered from Groupe Islamique Armé (GIA). The group formally pledged loyalty in September 2006 to Bin Ladin, changed its name in 2007, and wages regional low-level guerilla insurgency.

AL-NUSRAH FRONT

SYRIA

Al-Nusrah is one of the most dangerous and capable al-Qa'ida–affiliated groups operating in Syria and Lebanon. Since January 2012, the group announced its intentions to overthrow President Bashir al-Asad's regime and have mounted attacks against the regime and security targets in Syria and conducted suicide attacks against Lebanese Hizballah and Shia interests as well as security forces in Lebanon. The group's leader, Abu Muhammad al-Jawlani, in late September 2014 publicly called for retaliatory attacks against the US-led military coalition for airstrikes in Syria.

AL-MURABITUN

NORTH AND WEST AFRICA

Al-Murabitun is comprised of two former AQIM offshoots—veteran jihadist Mokhtar Belmokhtar's al-Mulathamun Battalion and al-Tawhid wa al-Jihad in West Africa (TWJWA)—which merged in August 2013. The group, whose name means "the sentinels," maintains an aggressive anti-Western agenda and seeks to "unite all Muslims from the Nile River to the Atlantic Ocean in violent jihad against Westerners."

AL-SHABAAB (HARAKAT SHABAAB AL-MUJAHIDIN)

لاإله إلاالله
الله
رسول
محمد

SOMALIA

Since 2006, terrorist and insurgent group al Shabaab has worked to remove Western influence from Somalia and establish an Islamic state. Al-Shabaab leadership is affiliated with al-Qa'ida and some are believed to have trained and fought in Afghanistan. The merger of the two groups was publicly announced in February 2012 by the now-deceased amir of al-Shabaab and Ayman al-Zawahiri, the leader of al-Qa'ida. Most of the group's fighters are predominantly interested in the nationalistic battle against the Somali Federal Government and not supportive of global violent jihad. Since 2013, al-Shabaab has launched high-profile operations in neighboring countries, most notably the attack on the Westgate Mall in Nairobi, Kenya in September 2013 and the attack against a restaurant in Djbouti popular with Westerners in May 2014.

ISLAMIC STATE OF IRAQ AND ASH-SHAM (ISIS), FORMERLY KNOWN AS AL-QA'IDA IN IRAQ (AQI)

لاإله إلاالله
الله
رسول
محمد

IRAQ, SYRIA, LEBANON

Abu Mus'ab al-Zarqawi in 2004 announced the group's affiliation with Bin Laden; it was renamed AQI to reflect the connection. Following al-Zarqawi's death in 2006, Abu Ayyub al-Masri took over and attempted to create a political front by publicly subordinating the group to the Islamic State of Iraq (ISI). The convictions in 2013 of two AQI-affiliated Iraqi refugees in Kentucky highlight a potential threat to the US from veteran AQI/ISIS fighters. ISIS in August 2014 beheaded an American journalist in Syria. The group has used suicide attacks against Lebanese Hizballah and Shia interests and Lebanese security forces in Lebanon, and in August 2014 kidnapped 11 security personnel and beheaded two others.

ABU SAYYAF GROUP (ASG)

SOUTHERN PHILIPPINES

ASG is the most violent Islamic separatist group promoting the independent Islamic state in western Mindanao and the Sulu Archipelago. Split from the Moro National Liberation Front in the early 1990s, ASG engages in bombings, assassinations, extortion, and kidnappings for ransom and has ties to Jemaah Islamiyah.

ANSAR BAYT AL-MAQDIS(ABM)

EGYPT

ABM is the most active and capable terrorist group operating in Egypt. It rose to prominence after the Egyptian revolution in 2011 when it began claiming responsibility for cross-border and rocket attacks into Israel and gas pipeline attacks in the Sinai. Since July 2013, ABM has focused its increasingly sophisticated and lethal attacks on the Egyptian Government and security forces. The group publicly pledged its allegiance to ISIS in November 2014.

BOKO HARAM

NIGERIA

ISIS-WA has existed in various forms since the late 1990s and seeks to overthrow the Nigerian Government and replace it with one based on Islamic law. Since 2011, ISIS-WA has conducted multiple attacks against a wide range of targets to include Christians, Nigerian security and police forces, media, schools, and politicians. The group's unprecedented levels of violence—including the kidnapping of 276 schoolgirls in Nigeria in April 2014—have brought international condemnation as well as collaboration on security initiatives by the US, UK, France, and African partners.

CONTINUITY IRISH REPUBLICAN ARMY(CIRA)

IRELAND

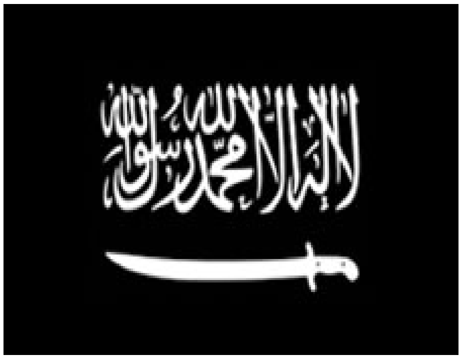
Founded in 1986, CIRA is the oldest Irish Republican dissident group and the only group that did not join New IRA, a coalition of terrorist organizations formed in July 2012. British authorities in early 2009 estimated the organization had a few dozen members. The most recent attack was in March 2013 when a member killed an individual responsible for another member's death.

HAMAS

GAZA STRIP AND WEST BANK

Hamas was established in the late 1980s during the first Palestinian uprising. The group maintains a military army, the Izz al-Din al-Qassam Brigades. HAMAS since July 2014 is at war with Israel.

IMIRAT KAVKAZ (IK OR CAUCASUS EMIRATE)



RUSSIA'S NORTH CAUCASUS

Founded in late 2007 by now-deceased Chechen violent extremist Doku Umarov, the IK is an Islamist militant organization aimed at liberating perceived Muslim lands from Russia. The group regularly conducts attacks against Russian security forces, although attacks declined in 2014, IK-associated personnel are also active in Syria.

JAISH-E-MOHAMMAD (JEM)

PAKISTAN

Founded in 2000 by Masood Azhar following his prison release in India. JEM’s aim is to unite Kashmir with Pakistan and expel foreign troops from Afghanistan. The group declared war against the US and operates openly in parts of Pakistan despite a ban on its activities in 2002.

JEMAAH ANSHORUT TAUHID (JAT)

INDONESIA

Radical cleric Abu Bakar Bashir founded the group in July 2008 to establish a caliphate in Indonesia. JAT leadership has publicly stated that violence is religiously permissible when directed against perceived enemies of Islam—specifically Indonesian judges, prosecutors, and police. JAT is implicated in a series of attacks conducted in 2011.

JEMAAH ISLAMIYA (JI)

INDONESIA

JI was formed in the early 1990s to establish an Islamic state in southern Thailand, Malaysia, Singapore, Indonesia, Brunei, and the southern Philippines. The group conducted a series of lethal bombings targeting Western interests in Indonesia and the Philippines during 2000-05, including attacks in 2002 against two nightclubs in Bali that killed 202 people, including seven Americans.

KURDISTAN PEOPLE'S CONGRESS OR KONGRA-GEL (KGK)

NORTHERN IRAQ AND SOUTHEASTERN TURKEY

Kurdish separatist group KGK is composed of mostly Turkish Kurds who in 1984 began a campaign of armed violence, including terrorism, resulting in more than 45,000 deaths. KGK has directed operatives to target security forces, government offices, and villagers who opposed it.

LASHKAR-E-TAYYIBA (LT)

KASHMIR, PAKISTAN

LT is the military wing of the Pakistan-based Islamic fundamentalist missionary organization established in the 1990s to oppose Soviets in Afghanistan. The group is one of the largest and most proficient Kashmir-focused militant groups. The Indian Government charged LT with the attacks in Mumbai in 2008, which killed more than 160 people. USPER David Coleman Headley admitted to attending LT training camps, pled guilty in March 2010 to surveying targets for LT attacks, and in January 2013 was sentenced to 35 years in prison.

FBI EXPLOSIVE UNIT:
(703) 632-7626 (tel: 703-632-7626) (8:00am – 5:00pm EST)
(202) 323-3300 (tel: 202-323-3300) (after hours)

HSIN:
https://hsin.dhs.gov (https://hsin.dhs.gov)

LEEP (LEO):
https://cjis.gov (https://cjis.gov)

STATE DEPARTMENT—PASSPORT OFFICE:
(877) 487-2778 (tel: 877-487-2778)

First responder agencies receiving citizen reports of lost or stolen passports should strongly encourage the reporting citizen to notify the US State Department of the missing passport so that the documents are not able to be used illicitly. Note that unless the State Department is notified by the person named on the passport, it will not be flagged/cancelled. The State Department will not accept third-party notifications, such as from the police agency taking the theft report.

Further information can be found at travel.state.gov (https://travel.state.gov).

(https://www.nctc.gov) **(https://www.dhs.gov)** **(https://www.fbi.gov)**

Office *of the*
Director *of* National Intelligence (https://www.dni.gov/index.php)

ODNI CENTERS

Cyber Threat Intelligence Integration Center (https://www.dni.gov/index.php/ctiic-home)

National Counterproliferation Center (https://www.dni.gov/index.php/ncpc-home)

National Counterintelligence and Security Center (https://www.dni.gov/index.php/ncsc-home)

National Counterterrorism Center (https://www.dni.gov/index.php/nctc-home)

ODNI OFFICES

Equal Employment Opportunity & Diversity (https://www.dni.gov/index.php/who-we-are/organizations/eeod/eeod-who-we-are)

IC Chief Human Capital Officer (https://www.dni.gov/index.php/who-we-are/organizations/chco/chco-who-we-are)

IC Inspector General (https://www.dni.gov/index.php/who-we-are/organizations/ic-ig/ic-ig-who-we-are)

Office of Civil Liberties, Privacy, and Transparency (https://www.dni.gov/index.php/who-we-are/organizations/clpt/clpt-who-we-are)

More Offices (https://www.dni.gov/index.php/who-we-are/organizations)

INFORMATION

Contact the IC IG (https://www.dni.gov/index.php/contact-the-icig)

No Fear Act (https://www.dni.gov/index.php/no-fear-act)

Privacy Policy (https://www.dni.gov/index.php/privacy-policy)

Customer Service (https://www.dni.gov/index.php/customer-service)

FOIA (https://www.dni.gov/index.php/foia)

USEFUL LINKS

For Kids (https://www.dni.gov/index.php/for-kids)

Ready.gov (http://www.ready.gov)

Open.gov (http://www.whitehouse.gov/open)

Flu.gov (http://www.flu.gov/)

Plain Language Act (https://www.dni.gov/index.php/plain-language-act)

Furlough Resources (https://www.dni.gov/index.php/furlough-resources)

ODNI Operating Status (https://www.dni.gov/index.php/odni-operating-status)

(https://service.govdelivery.com/accounts/USODNI/subscriber/new)
(https://www.dni.gov/index.php/rss) (http://www.icontherecord.tumblr.com/)
(https://www.twitter.com/odnigov) (http://www.facebook.com/dni.gov)
(http://www.flickr.com/photos/odnigov) (http://www.youtube.com/odnigov)
(http://www.scribd.com/odnigov) more (https://www.dni.gov/index.php/more)